TRUSTED FUTURE

ISSUE BRIEF

May 2022

CYBER THREATS FROM RUSSIA HIGHLIGHT THE NEED FOR TRUSTED CYBERSECURITY MEASURES

At a time of increasing global tensions, our national security experts are warning that cybersecurity threats from authoritarian regimes are on the rise. President Biden has warned our private sector leaders that now is the time to "accelerate efforts to lock their digital doors." Our expert agencies have urged businesses and organizations to take appropriate action. Here, we examine the heightened threat and highlight critical steps that businesses, tech users, and policymakers should take in this new environment.

A HEIGHTENED THREAT ENVIRONMENT CAUSED BY RUSSIA'S INVASION OF UKRAINE.

Russia's invasion of Ukraine earlier this year has heightened concern among experts and policy makers about the potential risk of offensive Russian cyber operations. Since the war's start, there have been serious and well-informed warnings that Russia could use cyber weapons in the invasion of Ukraine, and potentially against the West in response to sanctions imposed on Moscow. This included alerts from the Cybersecurity and Infrastructure Security Agency (CISA), the State Department, the Federal Bureau of Investigation (FBI), and even the president, as well as myriad independent analysts.

Based on recent public statements and warnings, however there is reason to believe that potential cyber threats are growing more serious. Cybersecurity authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom, known as the Five Eyes, recently released a joint Cybersecurity Advisory to warn that "evolving intelligence indicates that the Russian government is exploring options for potential cyberattacks (see the March 21, 2022, Statement by U.S. President Biden for more information). Recent Russian state-sponsored cyber operations have included distributed denial-of-service (DDoS) attacks, and older operations have included deployment of destructive malware against Ukrainian government and critical infrastructure organizations."

The Advisory also warns that "some cybercrime groups have recently publicly pledged support for the Russian government. These Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian government or the Russian people. Some groups have also threatened to conduct cyber operations against countries and organizations providing materiel support to Ukraine. Other cybercrime groups have recently conducted disruptive attacks against Ukrainian websites, likely in support of the Russian military offensive."

Microsoft also recently discovered at least six different Kremlin-linked hacking groups that have conducted nearly 240 cyber operations against Ukrainian targets.

INCREASED RISKS OF CYBER INTRUSIONS ARE LIKELY TO PERSIST FOR YEARS TO COME.

The Five Eyes advisory specifically attributes the increase of a potential threat to Russia's invasion of Ukraine and heightened tensions between Russia and the West. The suggestion that malware and DDoS attacks may be deployed in response to traditional tools of foreign policy, such as sanctions, suggests that Russia may be using the threat of cyber activity as a tool to counter the use of traditional means of enforcing acceptable international behavior. As a group of senior national security leaders, including Trusted Future's Advisory Board Member Admiral Michael Rogers, the former Director of the National Security Agency and Commander of CYBERCOM, recently highlighted:

> "This is a pivotal moment in modern history. There is a battle brewing between authoritarianism and democracy, and the former is using all the tools at its disposal, including a broad disinformation campaign and the threat of cyber-attacks, to bring about a change in the global order. We must confront these global challenges."

THIS NEW ENVIRONMENT EMPHASIZES THE NEED FOR RELIABLE AND TRUSTWORTHY SECURITY SOLUTIONS.

Our global digital ecosystem is under near constant threat from malicious actors using techniques that are becoming increasingly more complex, sophisticated, and ubiquitous. To take advantage of all the benefits of technology amid these emergent digital threats, users need to have trust in the security of technology systems. In order for there to be trust, the security needs to be placed at the core of any system.

Nation-states and criminal gangs are dedicated to finding and exploiting vulnerabilities. One of their most effective tools is the development of sophisticated new "social engineering" strategies to trick users into clicking on malevolent links, infected attachments, or downloading mobile malware directly onto devices. Even a small mistake can have far-reaching consequences. One example of the use of social engineering is the recent "FluBot"criminal campaign. In FluBot, the criminal sends a text message to a person pretending to be a package delivery company with information about your missing package. When the user clicks on the link, the link leads to a webpage that downloads malware onto the phone and allows the criminal to steal your banking and other information. The use of SMS messaging to gain access to devices and information on a smartphone is, called Smishing (the SMS/text version of phishing), and is on the rise. In our recent survey two-thirds of Americans reported on the receiving end of an attempted Smishing attack in the last year.

Sometimes malicious actors do not need such sophisticated tactics and exploit systems through other poor cyber hygiene practices. For example, the use of ransomware by criminals to extort money from the Colonial Pipeline company in 2021 that led to fuel shortages along the East Coast was accomplished through the exploit of one bad password. The criminals were able to gain access to the company's enterprise systems because one of Colonial's employees reused a password from another account that was already compromised. The compromised password associated with the employee was available on the dark web. That Colonial Pipeline system was not using multi-factor authentication, which left it exposed to penetration if just one login credential was obtained.

As information technology becomes more pervasive, devices more prolific, and the information we carry with us becomes more sensitive, the attack surface that hackers can attempt to exploit has increased substantially creating new kinds of potential harm. It means that as technology becomes increasingly central to our lives, making it secure and reliable from the start becomes ever more critical.

To elevate our cybersecurity posture, we need to focus on solutions across the ecosystem that embrace best practices, enable continuous innovation in cyber-defenses, advance globally and recognized frameworks, all underpinned by smart government policies to keep personal and business data secure and our economy moving forward.

Fundamental to this is embracing the concept of "security by design." Hardware manufacturers and software developers need to ensure their products are built and designed with security best practices, and individuals should include security considerations when assessing which products to buy. Businesses must emphasize security when running their enterprise networks. And policymakers must analyze the security implications at the outset when considering any changes to the policy or regulatory framework that governs the digital ecosystem.

IMPORTANT STEPS CAN BE TAKEN NOW.

In this heightened threat environment there are specific steps that businesses and organizations, individuals, and policymakers can take to prepare, respond, and mitigate against potential cyber intrusions. These include:

- **Businesses and organizations should follow CISA's Shields Up guidelines.** Every organization—large and small—must be prepared to respond to disruptive cyber incidents. CISA has provided guidance to help businesses and organizations develop a response plan. See their recommended actions here.

- **Individuals can better protect themselves and their organizations by practicing good cyber hygiene.** This includes using strong and unique passwords, multi-factor authentication (MFA), avoiding insecure websites, only downloading from official app stores, keeping software up to date, and responding to unsolicited messages with caution. For more information see Trusted Future's cyber hygiene tip sheet.

- **Policymakers should apply a 'security screen' to any legislative or regulatory proposals that could affect the digital ecosystem, and ensure up front that there would be no adverse national or economic security impacts from the proposals.** For example, a recent letter from leading bipartisan national security experts called on the congressional committees with national security jurisdiction to conduct a review "of any legislation that could hinder America's key technology companies in the fight against cyber and national security risks emanating from Russia's and China's growing digital authoritarianism." Employing this critical screen would help ensure that proposals do not have unintended consequences that could enhance adversaries' capabilities.


TRUSTED
FUTURE